REMARKS

Reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks is respectfully requested. This Amendment should be entered under Rule 116 because it places this application in condition for allowance.

By this Amendment, claims 1, 2, 7, 8, 10, 12, 14, 17, 21, and 23 are amended to correct minor typographical errors and do not raise any new issue requiring further search and/or consideration. Claims 17 and 21 are further amended to include the subject matter recited in claims 20 and 22, respectively, and claims 20 and 22 are herein canceled. Accordingly, claims 1-19, 21, and 23-26 are pending in this application.

35 USC §103(a) Rejections over Douglas in view of Pantuso are Traversed

The rejection of claims 1-11, 14-24, and 26 under 35 USC §103(a) as being unpatentable over Douglas (US PGPUB No. 20040049693) in view of Pantuso (US Patent No. 7,093,292) is respectfully traversed. The cancellation of claims 20 and 22, as indicated above, render the rejection of these claims moot.

Applicant respectfully submits that the combined disclosures of Douglas, Pantuso, and Katz do not teach or suggest all of Applicant's claimed features. Regarding independent claim 1, the Patent and Trademark Office (PTO) asserts that Pantuso, at column 4, lines 43-52; and column 6, lines 56-61) discloses "sending the central database from the computer network to an external support computer system for analysis of the entirety of the local event logs since a last analysis of the local event logs." Applicant respectfully disagrees.

At column 4, lines 43-52, Pantuso appears only to disclose a central server that receives information from fire-wall equipped computers, wherein "[o]nce the information is collected by the central server, the information is analyzed to ascertain intrusion activity in operation 304." Furthermore, at cited passage column 6, lines 56-61, Pantuso appears to only disclose a framework wherein a large number of firewalls may be used to collect intrusion activity information, and a central server can identify intrusion activity using information and push rules

to all of the firewalls to prevent the intrusion activity. Applicant respectfully submits that nowhere does Pantuso disclose, teach, or suggest sending the central database to an external support computer system for analysis of the entirety of the local event logs, as recited in claim 1.

Further, although Douglas appears to disclose an intrusion detection system (IDS) that further analyses the received data, Applicant respectfully submits that in paragraph [0002], Douglas teaches away from reporting ahead all detected packets, and instead suggests filtering packets to avoid overwhelming "a monolithic arrangement of 'mass detection and reporting.'" Specifically, at paragraph [0004] Douglas discloses passing all event data to a host computer that filters the data before passing the events to a second plurality of modules.

Therefore, Applicant respectfully submits that the asserted combination of references evidences no disclosure or motivation, implicit or explicit, to suggest "sending the central database from the computer network to an external support computer system for analysis of the entirety of the local event logs," as recited in claim 1.

Accordingly, Applicant respectfully submits that claim 1 is patentable due to the failure of Douglas in view of Pantuso to disclose, teach or motivate all recited features of claim 1. Independent claims 10 and amended claims 17, 21, and 23 incorporate the method of claim 1 and therefore are likewise patentable over the applied references.

Regarding independent claims 7 and 14, the PTO relies upon Pantuso, at column 4, lines 43-52, and column 6, lines 56-61, to disclose "wherein an entire[t]y of the local event logs are stored since a last analysis of the local event logs." Applicant respectfully disagrees and as presented above in regards to claim 1, submits that Pantuso not only discloses saving only filtered logs prior to being transmitted them to the IDS, thereby failing to disclose storing the entirety of the local event logs, but teaches away from the approach recited by Applicant.

Claims 2-6, 8, 9, 11, 18, 19, and 24-26 depend variously from independent claims 1, 10, 17, 21, and 23 and are likewise patentable over the asserted combination of references art for at least their dependence on an allowable base claim, as well as for the additional features they recite. Accordingly, withdrawal of the rejection of claims 1-11, 14-19, 21, and 23-26 over Douglas in view of Pantuso is respectfully requested.

Rejections under 35 USC §103(a) over Douglas in view of Pantuso and Katz are traversed

The rejection of claims 12, 13, and 25 under 35 USC §103(a) as being unpatentable over Douglas in view of Pantuso and further in view of Katz et al. ("Katz")(US Patent Application Publication No. 20020062259) is respectfully traversed.

Applicant respectfully submits that, as discussed above, claims 12, 13, and 25 are patentable over Douglas in view of Pantuso. The event handler of Katz likewise fails to disclose sending the central database from the computer network to an external support computer system for analysis of the entirety of the local event logs, as recited in independent claims 12 and 1, from which dependent claims 13 and 25 depend, respectively, therefrom.

Therefore, Applicants respectfully submit that the combination of Douglas, Pantuso, and Katz fails to disclose, teach or suggest all the features recited in claims 12, 13, and 25. Accordingly, claims 12, 13, and 25 are patentable over the asserted combination of references and withdrawal of the rejection is respectfully requested.

Conclusion

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 1-19, 21, and 23-26 are earnestly solicited.

The Examiner is invited to telephone the undersigned, Applicant's attorney of record, to facilitate advancement of the present application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 08-2025 and please credit any excess fees to such deposit account.

Respectfully submitted,

Bernd LABERTZ

Kenneth M. Berner

Kenneth M. Berner
Registration No. 37,093

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400
703-684-1111 Telephone
970-898-0640 Telecopier
Date: November 9, 2007
KMB/ERM/jlb